Ideal class groups, elliptic curves and zeta functions

Ming-Lun Hsieh

AS/NTU Basic Notion Seminar

June 15, 2020

Fermat's Last Theorem (∼1637)

Theorem (Wiles, et.al 1995)

Let $n > 2$ be an integer. For any non-zero integers X, Y, Z,

$$X^n + Y^n \neq Z^n.$$

In 1816, Gauss wrote: "**I confess that Fermat's Last Theorem, as an isolated proposition, has very little interest for me, because I could easily lay down a multitude of such propositions, which one could neither prove nor dispose of.**"

Wiles's proof was the culmination of decades of work in algebraic number theory, arithmetic geometry, and commutative algebra.

Kummer

In 1850, Kummer made the first progress towards Fermat Last Theorem. He proved that the equation $X^p + Y^p = Z^p$ has no non-trivial integral solution if p is a regular prime.

The idea of Kummer

For any positive integer n, let

$$\zeta_n = e^{2\pi\sqrt{-1}/n} = \cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n} \in \mathbf{C}$$

be a n-th primitive root of unity.

Consider the Fermat equation $X^p + Y^p = Z^p$ for a prime p. We have

$$X^p = (Z - Y)(Z - \zeta_p Y)(Z - \zeta_p^2 Y)\cdots(Z - \zeta_p^{p-1} Y).$$

If (X, Y, Z) is a non-trivial integral solution, Kummer observed that the common divisors of the linear factors $Z - \zeta_p^i Y$ are divisors of p in the ring $\mathbf{Z}[\zeta_p]$. He realized that if the ring $\mathbf{Z}[\zeta_p]$ have some property close to the unique prime factorization, then FLT may be solved.

Ideal class groups

If K is a finite extension of the rational number field $\mathbf{Q}$, denote by $\mathcal{O}_K$ the ring of integers of K. For example, $K = \mathbf{Q}(\sqrt{-5})$, then $\mathcal{O}_K = \left\{a + b\sqrt{-5} \mid a, b \text{ integers}\right\}$.

The ideal class group $\mathrm{Cl}(K)$ is defined to be

$$\mathrm{Cl}(K) = \{ \text{ the set of ideals of } \mathcal{O}_K \} / \sim .$$

Here we say $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a} = \alpha \cdot \mathfrak{b}$ for some $\alpha \in K^\times$.
The ideal class group $\mathrm{Cl}(K)$ is a finite group. We call the cardinality $h(K) := \#(\mathrm{Cl}(K))$ the class number of K.

Fact: $h(K) = 1$ if and only if

any element in $\mathcal{O}_K$ has a unique prime factorization.

Eg: $h(\mathbf{Q}) = 1$ and $h(\mathbf{Q}(\sqrt{-5})) = 2$.

Definition of regular primes

For each integer n, let $\mathbf{Q}(\zeta_n)$ be the finite extension of $\mathbf{Q}$ generated by ζ_n. We call $\mathbf{Q}(\zeta_n)$ the n-th cyclotomic field.

We say a prime p is regular if

$$p \text{ does not divide the class number } h(\mathbf{Q}(\zeta_p)).$$

Kummer proved that if p is a regular prime, then $X^p + Y^p = Z^p$ has no non-trivial integral solution.

Unfortunately, not all primes are regular. For example, $p = 691$ is not a regular prime, namely 691 divides $h(\mathbf{Q}(\zeta_{691}))$. The smallest non-regular prime is 37.

Conjecture (Siegel)

About 60.65% *of primes are regular.*

To compute the class number $h(\mathbf{Q}(\zeta_p))$, we need zeta functions.

Zeta values

The Riemann zeta function is defined by the series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

where s is a complex number with $\mathrm{Re}\,(s) > 1$.
Euler computed some values of $\zeta(s)$ at negative odd integers:

$$\zeta(-1) = -1/12, \quad \zeta(-3) = 1/120, \quad \zeta(-5) = -1/(2^2 \cdot 3^2 \cdot 7),$$
$$\zeta(-7) = 1/(2^4 \cdot 3 \cdot 5), \quad \zeta(-9) = -1/(2^2 \cdot 3 \cdot 11)$$

$$\zeta(-11) = 691/(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13), \ldots,$$
$$\zeta(-31) = -(37 \cdot 683 \cdot 305065927)/(2 \cdot 3 \cdot 5 \cdot 7), \ldots.$$

Note that 691 is a prime factor of

- the numerator of the zeta value $\zeta(-11)$ (analytic value);
- the class number $h(\mathbf{Q}(\zeta_{691}))$ (arithmetic value).

Similarly, 37 is a prime factor of

- the numerator of the zeta value $\zeta(-31)$;
- the class number $h(\mathbf{Q}(\zeta_{37}))$.

A refined relation

Let $A_p := \mathrm{Cl}(\mathbf{Q}(\zeta_p)) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ be the p-primary subgroup of $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$. Then A_p is equipped with a natural Galois action of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Let $\omega : \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \to \mathbf{Z}_p^\times$ be the unique character given by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$. We can decompose A_p into eigenspaces

$$A_p = \bigoplus_{k=0}^{p-1} A_p(k),$$

where $A_p(k) = \left\{x \in A_p \mid \sigma(x) = \omega^k(\sigma)x,\ \sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\right\}$. For $p = 691, 37$, one can prove a refined relation (Herbrand-Ribet Theorem)

$$691 \mid \zeta(-11); \quad 691 \mid \#(A_{691}(-11)).$$

$$37 \mid \zeta(-31); \quad 37 \mid \#(A_{37}(-31)).$$

The aim of Iwasawa theory is to provide a systematic treatment to understand the above phenomenon and the generalizations. Roughly speaking, classical Iwasawa theory studies the relation between

the ideal class group with Galois action $\Longleftrightarrow$ zeta values.

Dirichlet L-functions

In 1837, Dirichlet generalized Riemann's zeta function, and for a character $\chi : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{C}^\times$, he introduced the following complex L-function given by

$$L(s, \chi) = \sum_{n=1,\, p\nmid n}^{\infty} \frac{\chi(n)}{n^s}, \ \mathrm{Re}\, s > 1.$$

This function was invented by Dirichlet to show there are infinitely many primes in the arithmetic progression $\{pn + a\}_{n=1,2,\ldots}$ $(1 \leq a < p)$.

Zeta values = special values of Dirichlet L-functions

Dirichlet L-functions $L(s, \chi)$ has analytic continuation to the whole complex plane. If $\chi(-1) = -1$, then it is known that $L(0, \chi) \neq 0$ and

$$L(0, \chi) = \frac{1}{p} \sum_{a=1}^{p-1} \chi(a) a \in \overline{\mathbf{Z}}.$$

The p-adic character $\omega : \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \to \mathbf{Z}_p^\times$ can be viewed as a Dirichlet character $\omega : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{C}^\times$ in a natural way. In view of the above formula, we have $L(0, \omega^k) \in \mathbf{Z}_p$ for odd k.

The refined relation between ideal class number and zeta values

Theorem (Mazur-Wiles, 1984)

Let p be an odd prime. For any odd integer k, we have

$$\#(A_p(k)) = \#\left(\mathbf{Z}_p/(L(0,\omega^k))\right).$$

Remark

For any odd integer $k < 0$, we have the congruence relation

$$L(0,\omega^k) \equiv \zeta(k) \,(\mathrm{mod}\ p).$$

This explains our example with $p = 691$ and $k = -11$

$$691 \mid \zeta(-11) \iff 691 \mid L(0,\omega^{-11}) \iff 691 \mid \#(A_{691}(-11)).$$

Recall that p is regular if and only if $p \nmid \#(A_p)$. Since

$$A_p = \bigoplus_{k=0}^{p-1} A_p(k),$$

Mazur-Wiles' theorem shows that $\#(A_p(k))$ can be computed by Dirichlet L-values if k is odd. For even k, we have the following

Conjecture (Vandiver)

$$\#(A_p(k)) = 1 \text{ if } k \text{ is even.}$$

This conjecture has been verified for $p < 125000$.

Congruent number problem ($\sim$972 A.D.)

A positive square-free integer n is a congruent number if n is the area of a right-angled triangle with rational length sides. In other words, there exist positive rational numbers A, B, C such that

$$n = \frac{1}{2}AB, \quad C^2 = A^2 + B^2.$$

If A, B, C is a solution to the above equation, setting

$$x = C^2/4, \quad y = \frac{(A^2 - B^2)C}{2},$$

we see immediately that $(x, y) \in \mathbf{Q}^2$ is a rational solution of the cubic equation

$$y^2 = x(x - n)(x + n).$$

This is an example of elliptic curves!

Elliptic curves

Let $a, b \in \mathbf{Z}$ such that $\Delta := 4a^3 + 27b^2 \neq 0$. Let

$$f(X, Y, Z) = Y^2Z - (X^3 + aXZ^2 + bZ^3)$$

and let $E \subset \mathbf{P}^2$ be the zero set of F in $\mathbf{P}^2$, which defines a non-singular projective curve over $\mathbf{Q}$. For a field L, denote by $E(L)$ the set of L-rational points of E:

$$\begin{aligned} E(L) &= \left\{[a_0 : a_1 : a_2] \in \mathbf{P}^2(L) \mid f(a_0, a_1, a_2) = 0\right\} \\ &= \left\{(x, y) \in L^2 \mid y^2 = x^3 + ax + b\right\} \cup \{[0 : 1 : 0]\} \end{aligned}$$

We know

- $O := [0 : 1 : 0] \in E(\mathbf{Q})$.
- $E(\mathbf{C})$ is a Riemann surface of genus one.

We call (E, O) the elliptic curve over $\mathbf{Q}$ defined by the cubic equation $y^2 = x^3 + ax + b$.

Mordell-Weil theorem

We have an isomorphism

$$E(L) \simeq \mathrm{Pic}^0 E(L), \quad P \mapsto (P) - (O).$$

This gives an abelian group structure of $E(L)$.

Theorem (Mordell-Weil)

If L is a finite extension of $\mathbf{Q}$, then $E(L)$ is a finitely generated abelian group.

We call $\mathrm{rank}_{\mathbf{Z}} E(L)$ the algebraic rank of $E_{/L}$.

The congruent number problem and elliptic curves

For each positive integer n, we let $\mathcal{E}_n$ be the elliptic curve defined by the cubic equation $y^2 = x(x-n)(x+n)$.

Proposition

The integer n is a congruent number if and only if

$$\begin{aligned} \operatorname{rank}_{\mathbf{Z}} \mathcal{E}_n(\mathbf{Q}) > 0 &\iff \#(\mathcal{E}_n(\mathbf{Q})) = \infty \\ &\iff \mathcal{E}_n(\mathbf{Q}) \text{ contains a point of infinite order.} \end{aligned}$$

Finding non-torsion rational points in elliptic curves is difficult in general

Consider the elliptic curve

$$\mathcal{E}_{157} : y^2 = x(x + 157)(x - 157).$$

We can show that the torsion points are

$$\mathcal{E}_{157}(\mathbf{Q})_{\mathrm{tor}} = \{(0, 0), (157, 0), (-157, 0), [0 : 1 : 0]\}.$$

The simplest non-torsion point is given by (x_0, y_0) with

$$x_0 = \frac{957323593545015812583644 53}{27748778732924463216912 1}$$
$$y_0 = \frac{834062764128948944072857085701103222940}{14617254579172152656815525943819608 1}.$$

Finding this point requires a beautiful combination of tools from algebraic geometry, algebraic number theory and complex analysis.

The zeta function of $E/\mathbf{Q}$

If ℓ is a prime, let $\mathbb{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$ and define $a_\ell(E) \in \mathbf{Z}$ by

$$a_\ell(E) = \#(\mathbf{P}^1(\mathbb{F}_\ell)) - \#(E(\mathbb{F}_\ell)) = 1 + \ell - \#(E(\mathbb{F}_\ell)) \in \mathbf{Z}.$$

Define the zeta function of $E/\mathbf{Q}$

$$L(E/\mathbf{Q}, s) = \prod_{\ell \nmid \Delta} \frac{1}{1 - a_\ell(E)\ell^{-s} + \ell^{1-2s}} \quad (\operatorname{Re} s > \frac{3}{2}).$$

Theorem (Wiles et.al, 1995)

$L(E/\mathbf{Q}, s)$ has holomorphic continuation to the whole complex plane.

We call $\operatorname{ord}_{s=1} L(E/\mathbf{Q}, s)$ the analytic rank of E. Moreover, there is a unique positive integer N_E (the conductor of E) such that

$$\Lambda_E(s) := \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \cdot \Gamma(s) \cdot L(E/\mathbf{Q}, s)$$

satisfies the function equation

$$\Lambda_E(s) = w(E/\mathbf{Q}) \cdot \Lambda_E(2 - s), \quad w(E/Q) \in \{\pm 1\}.$$

A Millennium Prize Problem

Conjecture (Birch and Swinnerton-Dyer)

$$\mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) = \mathrm{ord}_{s=1} L(E/\mathbf{Q}, s).$$

Weak version of the conjecture:

$$\begin{aligned} L(E/\mathbf{Q}, 1) = 0 &\iff \mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) > 0 \\ &\iff E(\mathbf{Q}) \text{ has infinitely many points.} \end{aligned}$$

In our previous example $\mathcal{E}_{157}$, it is not difficult to show $L(\mathcal{E}_{157}/\mathbf{Q}, 1) = 0$.

Known results for the weak version

Theorem (Coates-Wiles, 1977; Kolyvagin, 1995)

$$\mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) = 0 \text{ if } \mathrm{ord}_{s=1} L(E/\mathbf{Q}, s) = 0.$$

In other words, $E(\mathbf{Q})$ is a finite group if $L(E/\mathbf{Q}, 1) \neq 0$.

Therefore, if $L(\mathcal{E}_n/\mathbf{Q}, 1) \neq 0$, then n is not a congruent number.

Theorem (Gross-Zagier, 1986; Kolyvagin, 1995)

$$\mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) = 1 \text{ if } \mathrm{ord}_{s=1} L(E/\mathbf{Q}, s) = 1.$$

The opposite implication

$$L(E/\mathbf{Q}, 1) = 0 \Rightarrow \mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) > 0$$

seems extremely difficult in general. Nonetheless, some conditional results can be obtained by Iwasawa theory for elliptic curves.

Tate-Shafarevich and Selmer groups for elliptic curves

The Tate-Shafarevich group $Ш(E/\mathbf{Q})$ is the class group of E defined by

$$Ш(E/\mathbf{Q}) = \{\text{isomorphism class } [C_{/\mathbf{Q}}] \mid C: \text{ genus one curve } C_{/\overline{\mathbf{Q}}} \simeq E_{/\overline{\mathbf{Q}}} \text{ and } C(\mathbf{Q}_\ell) \neq \emptyset \, \forall \text{ primes } \ell.\}$$

In terms of Galois cohomology groups,

$$Ш(E/\mathbf{Q}) = \ker \left\{ H^1(\mathbf{Q}, E) \to \prod_{\ell: \text{ primes}} H^1(\mathbf{Q}_\ell, E) \right\}.$$

Conjecture (Tate-Shafarevich)

$Ш(E/\mathbf{Q})$ *is a finite group.*

The Selmer group $Sel(E/\mathbf{Q})$ for $E/\mathbf{Q}$ is a discrete subgroup which fits into the following exact sequence

$$0 \to E(\mathbf{Q}) \otimes \mathbf{Q}/\mathbf{Z} \to Sel(E/\mathbf{Q}) \to Ш(E/\mathbf{Q}) \to 0.$$

Taking Pontryagin duals $(\bullet)^*$,

$$0 \to Ш(E/\mathbf{Q})^* \to Sel(E/\mathbf{Q})^* \to E(\mathbf{Q}) \otimes \widehat{\mathbf{Z}} \to 0.$$

Iwasawa theory for elliptic curves

Iwasawa theory for elliptic curves studies the p-adic variations of the Selmer group $Sel(E/\mathbf{Q})^*$ as well as the central L-value $L(E/\mathbf{Q}, 1)$.

This theory was initiated by Mazur in 1970, generalizing Iwasawa's ideas for ideal class groups to elliptic curves. The following is a result of efforts of four decades in Iwasawa theory for elliptic curves

Theorem (Rubin, 1991; Skinner-Urban, 2014)

Assume that $Ш(E/\mathbf{Q}) < \infty$. *Then*

$$L(E/\mathbf{Q}, 1) = 0 \Rightarrow \mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) > 0.$$

The case of CM abelian varieties

We can also formulate the BSD conjecture for any abelian variety $A_{/\mathbf{Q}}$ whenever the associated zeta functions $L(A/\mathbf{Q}, s)$ has the analytic continuation to $\mathrm{Re}\,(s) > 1^{-}$. In particular, this is known for abelian varieties with complex multiplications.
We used the arithmetic of Picard modular forms to study Iwasawa theory for CM fields and extended the above results to CM abelian varieties:

Theorem (H-, 2014)

Let $A_{/\mathbf{Q}}$ be a simple CM abelian variety. Assume that $Ш(A/\mathbf{Q}) < \infty$ Then

$$L(A/\mathbf{Q}, 1) = 0 \Rightarrow \mathrm{rank}_{\mathbf{Z}}\, A(\mathbf{Q}) > 0.$$

Theorem of Gross-Zagier, Kolyvagin and Skinner

Theorem (Gross-Zagier, Kolyvagin and Skinner)

$$\begin{aligned} &\mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) = 1 \quad \text{and} \quad Ш(E/\mathbf{Q}) < \infty \\ \Longleftrightarrow\ &\mathrm{ord}_{s=1} L(E/\mathbf{Q}, s) = 1. \end{aligned}$$

The key to the proof is the existence of Heegner points in addition to Iwasawa theory.
For each imaginary quadratic field K, the theory of complex multiplication produces a special point $P_K \in E(K) \otimes_{\mathbf{Z}} \mathbf{Q}$, which is called the Heegner point of E/K. Gross and Zagier proved

$$P_K \neq 0 \iff \mathrm{ord}_{s=1} L(E/K, s) = 1.$$

Using Iwasawa theory, Kolyvagin and Skinner proved that

$$P_K \neq 0 \text{ for some } K \iff \mathrm{rank}_{\mathbf{Z}}\, E(\mathbf{Q}) = 1 \text{ and } Ш(E/\mathbf{Q}) < \infty.$$

An analogue of Heegner points in the rank two case

Heegner points vanish if $\mathrm{rank}_{\mathbf{Z}} E(\mathbf{Q}) \geq 2$. It is desirable to find analogues of Heegner points for elliptic curves of higher ranks.

Inspired by recent works of Darmon and Rotger, we use Iwasawa theory for the triple product of modular forms to construct an element

$$\kappa_E \in E(\mathbf{Q}) \otimes_{\mathbf{Z}} \mathbf{Q}_p$$

under the the finiteness of Tate-Shafarevich groups. Unlike Heegner points, κ_E does not belong to $E(\mathbf{Q}) \otimes_{\mathbf{Z}} \mathbf{Q}$.

Theorem (Castella and H-, 2019)

Suppose that $Ш(E/\mathbf{Q}) < \infty$. *Then*

$$\kappa_E \neq 0 \iff \mathrm{rank}_{\mathbf{Z}} E(\mathbf{Q}) = 2.$$

The proof uses the construction of p-adic triple product L-functions and anticyclotomic Iwasawa theory for elliptic curves over imaginary quadratic fields.

Last example: Cursed curve ($\sim$1972)

Let $\mathcal{C} \subset \mathbf{P}^2$ be the plane curve over $\mathbf{Q}$ of defined to be the zero set of the homogenous polynomial of degree 4

$$F(X,Y,Z) = Y^4 + 5X^4 - 6X^2Y^2 + 6X^3Z + 26X^2YZ + 10XY^2Z \\ - 10Y^3Z - 32X^2Z^2 - 40XYZ^2 + 24Y^2Z^2 + 32XZ^3 - 16YZ^3.$$

The genus of $\mathcal{C}(\mathbf{C})$ is three, so $\#(\mathcal{C}(\mathbf{Q}))$ is finite by Faltings' theorem.

Theorem (Balakrishnan et.al, 2019)

$\mathcal{C}(\mathbf{Q})$ consists of the following seven points

$$\{[0:1:0],[0:0:1],[-1:0:1],[1:0:0],[1:1:0],[0:3:2],[1:0:1]\}.$$

The proof uses Chabauty-Kim method which crucially relies on the arithmetic structure of the étale and de Rham fundamental groups of X and theory of p-adic integration over one forms on curves.

Concluding remarks

The beauty of number theory stems from the *contradiction* between the simplicity of the problems and the complexity of the methods.

Moreover, the solutions usually exhibit the harmony between various branches of mathematics.

Thank you for your attention.